United Nations A/73/505

General Assembly

Distr.: General
19 November 2018

Original: English

**Seventy-third session**
Agenda item 96

# Developments in the field of information and telecommunications in the context of international security

## Report of the First Committee

*Rapporteur*: Ms. Muna Zawani **Md Idris** (Brunei Darussalam)

## I. Introduction

1. The item entitled "Developments in the field of information and telecommunications in the context of international security" was included in the provisional agenda of the seventy-third session of the General Assembly in accordance with Assembly decision 72/512.

2. At its 3rd plenary meeting, on 21 September 2018, the General Assembly, on the recommendation of the General Committee, decided to include the item in its agenda and to allocate it to the First Committee.

3. At its 1st meeting, on 4 October 2018, the First Committee decided to hold a general debate on all disarmament and international security items allocated to it, namely, items 93 to 108. Also at its 1st meeting, the Committee decided, on the basis of conference room papers before it,[1] on the final composition for the exchange with the High Representative for Disarmament Affairs and other high-level officials on the current state of affairs in the field of arms control and disarmament. At its 2nd to 11th meetings, from 8 to 12 and from 15 to 18 October, the Committee held a general debate on the items. At its 8th meeting, on 16 October, the Committee had an exchange with the High Representative on the follow-up to resolutions and decisions adopted by the Committee at previous sessions and on reports presented to the Committee for its consideration, with a special focus on the United Nations Institute for Disarmament Research. At its 10th meeting, on 17 October, the Committee had an exchange with the High Representative and other high-level officials on the current state of affairs in the field of arms control and disarmament. The Committee also held 15 meetings (11th to 25th), on 18 and 19, from 22 to 26 and from 29 to 31 October, for thematic discussions and panel exchanges with independent experts. At those

[1] A/C.1/73/CRP.2 and A/C.1/73/CRP.3, available at www.un.org/en/ga/first/73/documentation73.shtml.

18-19776 (E) 281118

Please recycle

meetings, as well as during the action phase, draft resolutions were introduced and considered. The Committee took action on all draft resolutions and decisions at its 26th to 31st meetings, on 1, 2, 5, 6 and 8 November.[2]

4. No documents were submitted for consideration under this item.

## II. Consideration of proposals

### A. Draft resolution A/C.1/73/L.27/Rev.1

5. On 8 November, the representative of the Russian Federation, on behalf of Algeria, Angola, Azerbaijan, Belarus, Bolivia (Plurinational State of), Burundi, Cambodia, China, Cuba, the Democratic People's Republic of Korea, the Democratic Republic of the Congo, Eritrea, Iran (Islamic Republic of), Kazakhstan, the Lao People's Democratic Republic, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Pakistan, the Russian Federation, Samoa, Sierra Leone, Suriname, the Syrian Arab Republic, Tajikistan, Turkmenistan, Uzbekistan, Venezuela (Bolivarian Republic of) and Zimbabwe, submitted a draft resolution entitled "Developments in the field of information and telecommunications in the context of international security" (A/C.1/73/L.27/Rev.1). Subsequently, Guinea, Kyrgyzstan and Myanmar joined in sponsoring the draft resolution.

6. At the 31st meeting, on 8 November, the Secretary of the Committee read out a statement by the Secretary-General concerning the financial implications of the draft resolution and reported that it superseded the statement of the programme budget implications of the draft resolution that had been issued as document A/C.1/73/L.71.

7. At the same meeting, the Committee adopted draft resolution A/C.1/73/L.27/Rev.1 by a recorded vote of 109 to 45, with 16 abstentions (see para. 11, draft resolution I). The voting was as follows:[3]

*In favour*:

Algeria, Angola, Argentina, Armenia, Azerbaijan, Bahrain, Bangladesh, Barbados, Belarus, Belize, Benin, Bhutan, Bolivia (Plurinational State of), Bosnia and Herzegovina, Brunei Darussalam, Burkina Faso, Burundi, Cabo Verde, Cambodia, Chad, China, Colombia, Costa Rica, Cuba, Democratic People's Republic of Korea, Djibouti, Dominican Republic, Ecuador, Egypt, El Salvador, Eritrea, Ethiopia, Gambia, Ghana, Guatemala, Guinea, Guinea-Bissau, Guyana, Honduras, India, Indonesia, Iran (Islamic Republic of), Iraq, Jamaica, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Lao People's Democratic Republic, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malaysia, Maldives, Mali, Mauritius, Mexico, Mongolia, Morocco, Mozambique, Myanmar, Namibia, Nepal, Nicaragua, Niger, Nigeria, Oman, Pakistan, Palau, Panama, Paraguay, Peru, Philippines, Qatar, Russian Federation, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, Saudi Arabia, Serbia, Seychelles, Singapore, Solomon Islands, South Africa, Sri Lanka, Sudan, Suriname, Syrian Arab Republic, Tajikistan, Thailand, Timor-Leste,

[2] For an account of the Committee's discussion of the item, see A/C.1/73/PV.1, A/C.1/73/PV.2, A/C.1/73/PV.3, A/C.1/73/PV.4, A/C.1/73/PV.5, A/C.1/73/PV.6, A/C.1/73/PV.7, A/C.1/73/PV.8, A/C.1/73/PV.9, A/C.1/73/PV.10, A/C.1/73/PV.11, A/C.1/73/PV.12, A/C.1/73/PV.13, A/C.1/73/PV.14, A/C.1/73/PV.15, A/C.1/73/PV.16, A/C.1/73/PV.17, A/C.1/73/PV.18, A/C.1/73/PV.19, A/C.1/73/PV.20, A/C.1/73/PV.21, A/C.1/73/PV.22, A/C.1/73/PV.23, A/C.1/73/PV.24, A/C.1/73/PV.25, A/C.1/73/PV.26, A/C.1/73/PV.27, A/C.1/73/PV.28, A/C.1/73/PV.29, A/C.1/73/PV.30 and A/C.1/73/PV.31.

[3] Subsequently the delegation of the Democratic Republic of Congo indicated that it had intended to vote in favour.

Togo, Tunisia, Turkmenistan, Uganda, United Arab Emirates, United Republic of Tanzania, Uruguay, Uzbekistan, Vanuatu, Venezuela (Bolivarian Republic of), Viet Nam, Yemen, Zambia, Zimbabwe.

*Against*:

Albania, Andorra, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America.

*Abstaining*:

Antigua and Barbuda, Bahamas, Botswana, Brazil, Chile, Côte d'Ivoire, Equatorial Guinea, Fiji, Haiti, Papua New Guinea, Republic of Korea, Republic of Moldova, Rwanda, Senegal, Switzerland, Turkey.

## B. Consideration of draft resolution A/C.1/73/L.37

8. On 18 October, the representative of the United States of America, on behalf of Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malawi, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, the United Kingdom of Great Britain and Northern Ireland and the United States of America, submitted a draft resolution entitled "Advancing responsible State behaviour in cyberspace in the context of international security" (A/C.1/73/L.37). Subsequently, Albania, Chile, the Democratic Republic of the Congo, Guinea, Iceland, Liechtenstein, Montenegro, New Zealand, Norway, the Republic of Korea, the Republic of Moldova, Samoa, Sierra Leone, the former Yugoslav Republic of Macedonia and Turkey joined in sponsoring the draft resolution.

9. At the 31st meeting, on 8 November, the Secretary informed the Committee that a statement of the programme budget implications of the draft resolution had been issued as document A/C.1/73/L.72.

10. At the same meeting, the Committee adopted draft resolution A/C.1/73/L.37 by a recorded vote of 139 to 11, with 18 abstentions (see para. 11, draft resolution II). The voting was as follows:[4]

*In favour*:

Afghanistan, Albania, Andorra, Antigua and Barbuda, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belgium, Belize, Benin, Bhutan, Bosnia and Herzegovina, Brazil, Brunei Darussalam, Bulgaria, Burkina Faso, Cabo Verde, Canada, Chad, Chile, Colombia, Congo, Costa Rica, Croatia, Cyprus, Czechia, Denmark, Djibouti, Dominican Republic, Ecuador, El Salvador, Eritrea, Estonia, Ethiopia, Finland, France, Gambia, Georgia, Germany, Ghana, Greece, Guatemala, Guinea, Guinea-Bissau, Guyana, Haiti, Honduras, Hungary, Iceland, India, Indonesia, Iraq, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Latvia, Lesotho, Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Madagascar, Malaysia, Maldives, Mali, Malta, Marshall Islands, Mauritius,

[4] Subsequently the delegation of the Democratic Republic of Congo indicated that it had intended to vote in favour, and the delegations of Mozambique and Pakistan indicated that they had intended to abstain.

Mexico, Micronesia (Federated States of), Monaco, Mongolia, Montenegro, Morocco, Mozambique, Nepal, Netherlands, New Zealand, Niger, Nigeria, Norway, Oman, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Republic of Korea, Republic of Moldova, Romania, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, San Marino, Saudi Arabia, Serbia, Seychelles, Singapore, Slovakia, Slovenia, Solomon Islands, South Africa, Spain, Sri Lanka, Sudan, Sweden, Switzerland, Tajikistan, Thailand, the former Yugoslav Republic of Macedonia, Togo, Tunisia, Turkey, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United Republic of Tanzania, United States of America, Uruguay, Vanuatu, Viet Nam, Yemen, Zambia.

*Against*:

Bolivia (Plurinational State of), China, Cuba, Democratic People's Republic of Korea, Egypt, Iran (Islamic Republic of), Nicaragua, Russian Federation, Syrian Arab Republic, Venezuela (Bolivarian Republic of), Zimbabwe.

*Abstaining*:

Algeria, Angola, Belarus, Botswana, Burundi, Cambodia, Côte d'Ivoire, Equatorial Guinea, Fiji, Lao People's Democratic Republic, Lebanon, Myanmar, Namibia, Palau, Papua New Guinea, Rwanda, Senegal, Uganda.

# III. Recommendation of the First Committee

11. The First Committee recommends to the General Assembly the adoption of the following draft resolutions:

## Draft resolution I
## Developments in the field of information and telecommunications in the context of international security

*The General Assembly*,

*Recalling* its resolutions 36/103 of 9 December 1981, 43/78 H of 7 December 1988, 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 5 December 2016,

*Noting* that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

*Underscoring* the aspirations of the international community to the peaceful use of information and communications technologies (ICTs) for the common good of humankind and to further the sustainable development of all countries, irrespective of their scientific and technological development,

*Noting* that capacity-building is essential for cooperation of States and confidence-building in the field of ICT security,

*Recognizing* that some States may require assistance in their efforts to bridge the divide in the security of ICTs and their use,

*Noting* that providing assistance, upon request, to build capacity in the area of ICT security is essential for international security,

*Affirming* that capacity-building measures should seek to promote the use of ICTs for peaceful purposes,

*Confirming* that ICTs are dual-use technologies and can be used for both legitimate and malicious purposes,

*Expressing concern* that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely,

*Stressing* that it is in the interest of all States to promote the use of ICTs for peaceful purposes, with the objective of shaping a community of shared future for humankind in cyberspace, and that States also have an interest in preventing conflict arising from the use of ICTs,

*Noting* that the United Nations should play a leading role in promoting dialogue among Member States to develop common understandings on the security of and the use of ICTs, as well as in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour in this sphere, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices,

*Expressing concern* that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security,

*Considering* that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

*Underlining* the importance of respect for human rights and fundamental freedoms in the use of ICTs,

*Welcoming* the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General,[1]

*Welcoming also* that, in considering the application of international law to State use of ICTs, the Group of Governmental Experts, in its 2015 report,[2] identified as of central importance the commitments of States to the following principles of the Charter of the United Nations and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States,

*Confirming* the conclusions of the Group of Governmental Experts, in its 2013[3] and 2015[2] reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of ICTs can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

*Confirming also* that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory,

*Reaffirming* the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations,

*Recognizing* the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States,

*Stressing* that, while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations,

1. *Welcomes* the following set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and

[1] A/65/201, A/68/98 and A/70/174.
[2] A/70/174.
[3] A/68/98.

Telecommunications in the Context of International Security of 2013[3] and 2015[2] adopted by consensus and recommended in resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security", adopted by the General Assembly on 5 December 2016:

1.1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

1.2. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

1.3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.

1.4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

1.5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 of 5 July 2012[4] and 26/13 of 26 June 2014[5] on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

1.6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

1.7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

1.8. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

[4] See *Official Records of the General Assembly, Sixty-seventh Session, Supplement No. 53* and corrigendum (A/67/53 and A/67/53/Corr.1), chap. IV, sect. A.

[5] Ibid., *Sixty-ninth Session, Supplement No. 53* (A/69/53), chap. V, sect. A.

1.9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

1.10. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

1.11. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

1.12. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

1.13. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role;

2. *Calls upon* Member States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

3. *Considers* that the purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

4. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,[1] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 3 above;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

5. *Decides* to convene, beginning in 2019, with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent, an open-ended working group acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as

confidence-building measures and capacity-building and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-fifth session, and to provide the possibility of holding, from within voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate;

6. *Also decides* that the open-ended working group shall hold its organizational session in June 2019 in order to agree on the organizational arrangements connected with the group;

7. *Further decides* to include in the provisional agenda of its seventy-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

## Draft resolution II
## Advancing responsible State behaviour in cyberspace in the context of international security

*The General Assembly*,

*Recalling* its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 5 December 2016, as well as its decision 72/512 of 4 December 2017,

*Noting* that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

*Affirming* that it sees in this progress the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

*Noting* that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

*Confirming* that information and communications technologies are dual-use technologies and can be used for both legitimate and malicious purposes,

*Stressing* that it is in the interest of all States to promote the use of information and communications technologies for peaceful purposes and to prevent conflict arising from the use of information and communications technologies,

*Expressing concern* that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States, to the detriment of their security in both civil and military fields,

*Underscoring* the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies,

*Underlining* the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies,

*Welcoming* the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the 2010,[1] 2013[2] and 2015[3] reports transmitted by the Secretary-General,

*Stressing* the importance of the assessments and recommendations contained in the reports of the Group of Governmental Experts,

*Confirming* the conclusions of the Group of Governmental Experts, in its 2013 and 2015 reports, that international law, and in particular the Charter of the United

[1] A/65/201.
[2] A/68/98.
[3] A/70/174.

Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

*Confirming also* the conclusions of the Group of Governmental Experts that voluntary confidence-building measures can promote trust and assurance among States and help to reduce the risk of conflict by increasing predictability and reducing misperception and thereby make an important contribution to addressing the concerns of States over the use of information and communications technologies by States and could be a significant step towards greater international security,

*Confirming further* the conclusions of the Group of Governmental Experts that providing assistance to build capacity in the area of information and communications technology security is also essential for international security, by improving the capacity of States for cooperation and collective action and promoting the use of such technologies for peaceful purposes,

*Stressing* that, while States have a primary responsibility for maintaining a secure and peaceful information and communications technology environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations,

1. *Calls upon* Member States:

(a) To be guided in their use of information and communications technologies by the 2010,[1] 2013[2] and 2015[3] reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security;

(b) To support the implementation of cooperative measures, as identified in the reports of the Group of Governmental Experts, to address the threats emerging in this field and ensure an open, interoperable, reliable and secure information and communications technology environment consistent with the need to preserve the free flow of information;

2. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts, to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(b) The content of the concepts mentioned in the reports of the Group of Governmental Experts;

3. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in the above-mentioned reports, to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States, and to submit a report on

the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session;

4. *Requests* the Office for Disarmament Affairs of the Secretariat, through existing resources and voluntary contributions, on behalf of the members of the group of governmental experts, to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations, to convene a series of consultations to share views on the issues within the mandate of the group in advance of its sessions;

5. *Requests* the Chair of the group of governmental experts to organize two two-day informal consultative meetings, open-ended so that all Member States can engage in interactive discussions and share their views, which the Chair shall convey to the group of governmental experts for consideration;

6. *Decides* to include in the provisional agenda of its seventy-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".